View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Queensland University of Technology ePrints Archive

Queensland University of Technology
Brisbane Australia

This is the author's version of a work that was submitted/accepted for publication in the following source:

Salehi Shahraki, Ahmad, Razzaque, M.A., Naraei, Parisa, & Farrokhtala, Ali
(2013)
Detection of sinkhole attack in wireless sensor networks. In
IEEE International Conference on Space Science and Communication (IconSpace), IEEE, Melaka, pp. 361-365.

This file was downloaded from: https://eprints.qut.edu.au/74463/

© Copyright 2013 IEEE

Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Notice: *Changes introduced as a result of publishing processes such as copy-editing and formatting may not be reflected in this document. For a definitive version of this work, please refer to the published source:*

https://doi.org/10.1109/IconSpace.2013.6599496

Detection of Sinkhole Attack in Wireless Sensor Networks

Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala
Faculty of Computing
Universiti Technologi of Malaysia (UTM),
Skudai, Malaysia
ahmad.salehi.sh@gmail.com, marazzaque@utm.my,
{parisa.naraei, farrokhtala}@gmail.com

***Abstract*— Generally wireless sensor networks rely of many-to-one communication approach for data gathering. This approach is extremely susceptible to sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information, and subsequently presents selective forwarding or change the data that carry through it. A sinkhole attack causes an important threat to sensor networks and it should be considered that the sensor nodes are mostly spread out in open areas and of weak computation and battery power. In order to detect the intruder in a sinkhole attack this paper suggests an algorithm which firstly finds a group of suspected nodes by analyzing the consistency of data. Then, the intruder is recognized efficiently in the group by checking the network flow information. The proposed algorithm's performance has been evaluated by using numerical analysis and simulations. Therefore, accuracy and efficiency of algorithm would be verified.**

Keywords*— *Wireless Sensor Networks, Sinkhole Attack, Intruder Detection, security in wireless sensor networks, Detection of sinkhole attack.

I. INTRODUCTION

Wireless sensor networks (WSNs) have grown in importance as a low-cost solution for data measurement and collection. A key advantage of WSNs is their ease of deployment, in part due to their use of routing protocols that self-configure the network [1, 2]. However, if WSNs are to be used to monitor critical infrastructure, such as water distribution, then it is essential that the integrity of the WSN be protected against malicious attacks. In particular, the routing protocols used with WSNs are potentially vulnerable to routing attacks, which can disrupt connectivity in the network. While traditional cryptographic defenses are used to protect wired networks, the limited communication and Central processing unit resources in low-cost wireless sensor nodes makes resource intensive cryptography impractical.

Sinkhole attacks (see Fig. 1) typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high quality route to a BS. Some protocols might actually try to verify the quality of route with end-to-end acknowledgements containing reliability or latency information. In this case, a laptop-class adversary with a powerful transmitter can actually provide a high quality route by transmitting with enough power to reach the BS in a single hop, or by using a wormhole attack.

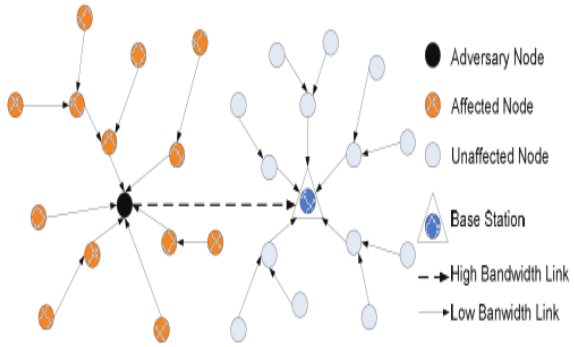

Figure 1: Sinkhole Attack

Due to either the real or imagined high quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a BS through the adversary, and also propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large "sphere of influence", attracting all traffics destined for a BS from nodes several hops away from the compromised node.

The base station is prevented by the sinkhole attack from achieving complete and accurate sensing data, and therefore it is resulted in an important threat which is critical for wireless sensor networks. In fact, this happens due to the unprotected wireless links, the deployment of the sensors in open areas, and the weak computation and battery power.

The current routing protocols in sensor networks show usually vulnerability to the sinkhole attack [1]. Some studies have suggested several secure mechanisms to use as cryptographic methods for protecting network however, they

are mostly localized, or there is a high computation and also a requirement for time synchronization among the nodes. We present a new lightweight algorithm in order to detect the sinkhole attack and to recognize the engaged intruder [3, 9].

This paper considers a usual many-to-one communication where the routes are set up based on the receiving of route advertisements. The suggested method can investigate the asymmetricity between the sensor nodes and the base station. This solution causes also effective application of the relatively-high computation and communication power of the base station [4, 7].

Two main parts can be explained for this technique; a secure and low-overhead algorithm and an efficient identification algorithm. The first one is a protected and low-overhead algorithm for the base station which can collect the network flow information from the attacked area. The second one is an algorithm able to analyze the routing pattern and identify the intruder.

This paper also focuses on the complex scenario with colluding nodes that can as a group, deceive the base station about the location of intruder. Particularly, multiple suspected nodes are checked and the intruder is recognized with a voting method.

It is demonstrated that the suggested algorithm is accurate as long as the normal nodes are main. Simulations are used to evaluate the performance of the presented algorithm, and the effectiveness and accuracy of the algorithm are verified.

II. RELATED WORKS

One of the important topics in the Internet evolution research is intrusion detection [6]. In addition, several studies have suggested various detection algorithms for wireless ad hoc networks. It is supposed that there are uniform nodes and symmetric data communication patterns among the nodes [7, 8]. However, there are various problems specifically the sinkhole attack for one-to-many communication pattern in wireless sensor networks. And this problem is being harmful due to the feeble computation and battery power of the sensor nodes. Although Karlof used a trust scheme to the routing protocol for detection of sinkhole and wormhole attacks in a sensor network, however activity of nodes in a promiscuous mode is essential. It has been shown that packet leash can confide the maximum transmission time and distance of each packet [8]. It is suggested that a key can be acquired by a node for any other node and each data packet can use authentication.

Ngai et al. [1] firstly has suggested a method for detection of sinkhole attacks which includes the BS in the detection process, causing an elevated communication cost for the protocol. The network is flooded by the BS with a request message including the IDs of the influenced nodes. The affected nodes reply to the BS with a message containing their IDs, ID of the next hop and the associated cost. The received information is then used from the BS to construct a network flow graph for identifying the sinkhole. Other existing protocols build detecting mechanisms for sinkhole attacks in sensor networks that are based on routing protocols usually deployed in Ad-Hoc networks, like the Ad Hoc On-demand Distance Vector Protocol (AODV) [6] and the Dynamic Source Routing (DSR) Protocol [8]. In our experience, the routing protocols are specifically designed for sensor networks, like MintRoute and MultiHopLQI, require much less resources and are usually preferred for such networks.

As mentioned earlier, this commonly used many-to-one communication pattern is vulnerable to sinkhole attacks. In this type of attack, an intruder usually attracts network traffic by advertising itself as having the shortest path to the base station. For example, as shown in Fig. 1a, an intruder, which is equipped with much higher computation and communication power than a normal sensor node, creates a high-quality single-hop link to the BS. It can then advertise imitated routing messages about the high quality route, spoofing the surrounding nodes to create a sinkhole (SH). A sinkhole can also be performed using a wormhole, which creates a metaphorical sinkhole with the intruder being the center; the intruder then relays the messages received in one part of the network toward the sink using a tunnel (see Fig. 2b).

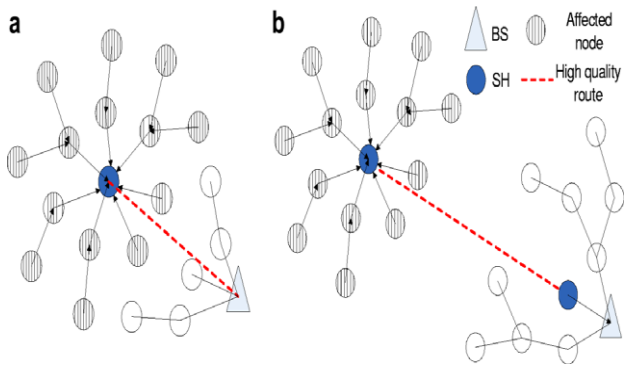

Figure 2: (a) Using an artificial high quality route; (b) using a wormhole.

III. ASSUMPTION AND NETWORK MODEL

In a wireless sensor network, multiple nodes would send sensor readings to a BS for further processing. It is known that such a many-to-one communication is highly vulnerable to a sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information, and then performs selective forwarding or alters the data passing through it [5]. A sinkhole attack forms a serious threat to sensor networks, particularly considering that the sensor nodes are often deployed in open areas and of weak computation and battery power. Although some secure or geographic based routing protocols resist to the sinkhole attacks in certain level, many current routing protocols in sensor networks are susceptible to the sinkhole attack.

It is supposed that the sensor nodes are either normal or malicious. The sinkhole attack center is a malicious node which is compromised by the intruder. It should be noticed that if there is only one compromised node, many surrounding normal nodes can be affected by this one compromised node via making a high quality route to the base station. In addition, this intruder can also collude with some other malicious nodes.

They are able to even cooperatively deceive the detection algorithm by proposing a normal node as the intruder.

IV. SINKHOLE ATTACK DETECTION

In this section, we show how find a sinkhole attack in wireless sensor network, and after that how identify the intruder in area. The purpose of adversary in a sinkhole attack is to tempt almost all the traffic from a special network by way of a compromised node, making a metaphorical sinkhole with the adversary at the base station. Normally, by making a compromised node which appeared to be particularly interesting to encircling nodes concerning the routing algorithm, sinkhole attacks can act. Since of difficulty to confirm routing information which provided by a node, sinkhole attacks are difficult to counter. For instance, laptop class adversary has a great power radio transmitter. This permits laptop-class adversary to supply a high-quality route by transmitting with adequate power to obtain a broad area of the network.

At the first, we focus on single malicious node and then enhance it to find multiple malicious nodes in next section. So, the algorithm first finds a list of suspected nodes through checking data consistency, and then effectively identifies the intruder in the list through analyzing the network flow information. The algorithm is also robust to deal with multiple malicious nodes that cooperatively hide the real intruder.

a) Estimate the attacked area: Firstly to gather the network flow information from the attacked area, a safe and low-overhead algorithm for the base station is used and in the second, to investigate the routing pattern and positions the intruder an effective identification algorithm is employed. The complicated story with cheating nodes which collectively deceive the destination about the invader condition is regarded too. We continue two methods to find an intruder in sinkhole attack.

First of all, by calculating the area of attack the network is arranged into several under-domains and information within every of them are compared. The attack also can be discovered through the detection of the changeable data among the typical sensors and assault nodes in the under-domains. Moreover to explore the losing data of the attacked sensor and to recognize the area of attack it can be used. An intruder cannot change the data starting in all the nodes in the network due to the size limitation of the attacked area.

For demonstrate, perceive a supervision application in from what sensor nodes give in data to the base station frequently. Let X_1 , X_2 … X_n and Y_1 , Y_2 ... Y_n and ∂_1 , ∂_2 ...∂_n be the sensing data collected.

$$(\delta)^2 = \sum_{i=1}^{m} \frac{(\delta i \pm \sqrt{((X - Xi)^2 + (Y - Yi)^2)})^2}{m}$$

Therefore, in some of the sub-areas the attack has to be found. Following the recognition of a group of suspicious nodes, the location of sinkhole can be calculated by using the BS. Particularly, an ability attacked area that includes any suspicious nodes can be encircled. Second, the area of attack can include lots of nodes, and in a multi-hop sensor network the sinkhole is not inevitably the center of the area, also it is not essential to more identify the accurate intruder and isolate it from the network. For finding the intruder: It is attainable by examining the routing model in the influenced domain. So, a technique which gathers the network into data to make easier the routing model examination is shown (Fig.3).

BS	Base station
SH	Sinkhole attack

Table 1: Abbreviations

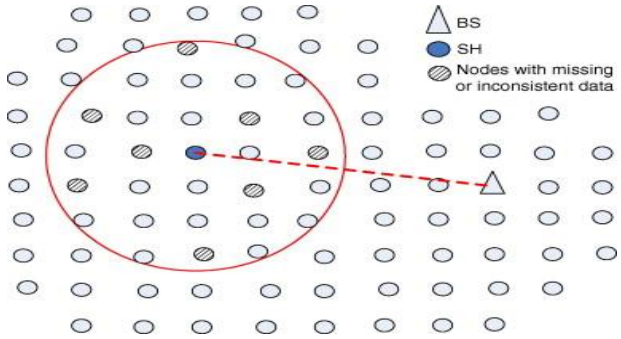

Figure 3: Estimate the attacked area

b) Identify by intruder: The message has within the identity of the influenced nodes. At the beginning, a request message goes into the BS. The message has IDs of the influenced nodes which flooding hop by hop. Since there is every node‘s ID, the request is accepted by all nodes and they should reply the BS by messages that contain their own ID; the next-hop node. Note that the next-hop and the cost could already. Pay attention for the attack which could influence the next-hop and the cost previously. So, the reply message should be transferred through the reverse path in the flooding, which relates to the original route without intruding.

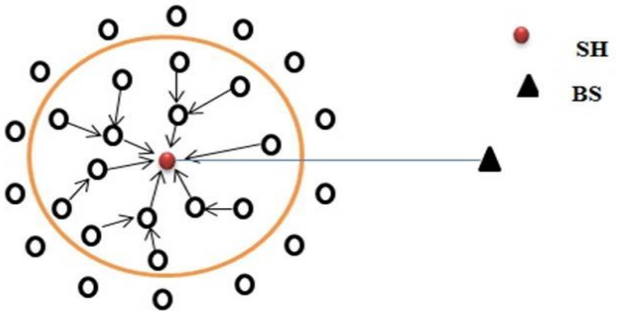

Figure 4: Network into the attack area

V. PERFORMANCE EVALUATION

The performance of suggested sinkhole detection algorithm is further evaluated by simulating a wireless sensor network with a 150 meter by 150 meter field in which 200 nodes are placed with uniform random distribution. The sensors adopt IEEE 802.11 MAC protocol with of 5 meter. In order to collect data from the sensors a base station is placed at the center of the network. Furthermore, a sinkhole attack a sinkhole is added to the network at x- and y-coordinates (50, 50) in order to emulate. It is important to evaluate the accuracy on intruder identification.

Number of nodes	200
Number of sinkhole	1
Message drop rate (d)	0.8
Packet size	500
Traffic Type	GBR
Location of sinkhole	(35, 35)
Location of BS	(80, 80)
Transmission range	100m
Protocol	AODV
Malicious node	1
Movement Model	Random Way point

Table 2: Parametrs for simulation

a) accuracy of intruder identification: The accuracy of suggested intruder detection algorithm for sinkhole attacks is investigated in the first set of experiments and three measures are considered including; (1) success rate, which shows the ability of the presented algorithm to properly recognize the SH in percentage; (2) false-positive rate, which shows the ability of suggested algorithm to incorrectly identify the SH; and (3) false-negative rate, which shows the inability of algorithm in identification of intruder which is in fact exist.

Figure 5 shows the success rate of intruder identification. The figure show that algorithm work in best situation when m is less than 50% of colluding nodes in dropping rate = 0.8. When dropping rate increase we can see that dropping rate drop. This means we have some missing data in networks.

Figure 6 and 7 show the false positive rate and false negative rate of colluding nodes. When the false negative increase in the networks we can see our algorithm works well but in false positive rate is reverse. When the colluding nodes increase the false positive increase slightly to reach 23 of false positive rate.

According to above results, it is show that our algorithm can effective related the previous works [1, 2, and 5] in m=50%. In the Success rate in intruder identification, our algorithm detect the intruder in highest rate in 50% of colluding nodes, but the accuracy is 79% in end; however, the rate of colluding nodes in [2] is a bit less than new results. The similar results are show in Figure 6 and 7. This show that our result is effective relative previous works in m=50% of colluding nodes.

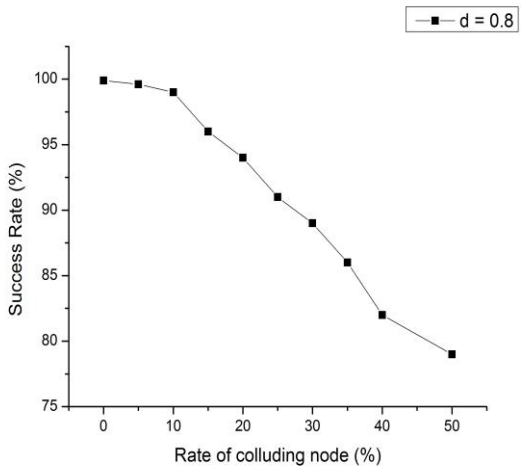

Figure 5: Success rate in intruder identification

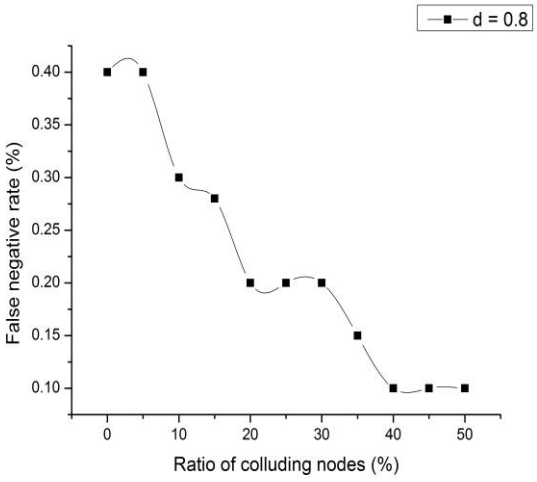

Figure 6: False negative rate in intruder identification

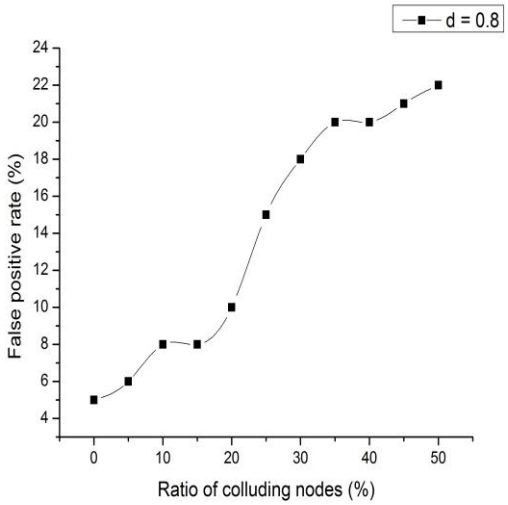

Figure 7: False positive rate in intruder identification

VI. CONLUSION AND FUTURE WORK

This study suggested a worthwhile technique to identify sinkhole attack in a wireless sensor network and the algorithm is composed of two steps. At the first the algorithm locates a list of suspected nodes by testing consistency of data. Then the intruder in the list is recognized via analyzing the network flow information. Moreover, the study has investigated the algorithm performance via numerical analysis and simulations. As a result, the effectiveness and accuracy of the algorithm have been demonstrated at the result in last section. This study can be further improved specifically in greater effective statistical algorithms to recognize inconsistency of data. Therefore they can correctly locate suspected nodes in sinkhole attacks and can identify communication and computation overhead.

REFERENCES

[1] Ngai, E. C. H., Liu, J. and Lyu, M. R. On the intruder detection for sinkhole attack in Wireless Sensor networks. IEEE communication Society matter expert.. Published in IEEE 2006. June. Canada. 3383-3389.

[2] Ngai, E. C. H., Liu, J. and Lyu, M. R. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer communication. 6 May, 2007. Elsevier locate. 2353-2364

[3] Choi, B. G., Cho, H. E., Hong, C. S. and Kim, J. H. A sinkhole Attack detection Mechanism for LQI based Mesh Routing in Wireless Sensor Networks. International confrance wireless security. 21-24 january (2008). Korea. 65-8

[4] Nisarg. G, Rahila. P. Review on Sinkhole Detection Techniques in Mobile Adhoc Network. Dep. K (Ed.). International Conference on Soft Computing for Problem Solving. (2012). (pp. 535-548). India: Springer India.

[5] Sharmila, S. and Umammaheswari, G. Detecting of sinkhole attack in Wireless Sensor networks using Message Digest Algorithms. International confrance in IEEE. May 12-14 (2011).75-80

[6] Teng, Liping. And Zhang, Y. SeRA: Secure Routing Algorithm against Sinkhole attacks for Mobile Wireless Sensor Networks. Second International Conference on computer Modeling and Simulation. 22-24 January (2010). ICCCMS. IEEE. 79-82.

[7] Sheela, D., Kumar, C. N. and Mahadeven, G. A non-Cryptographic method Of Sinkhole Attack Detecting In Wireless Sensor Networks. IEEE International Confrance On recent Trend in Information Technology. June 3-5(2011). MIT, Anna University.527-532.

[8] Karlof, C. and Wagner, D. Secure Routing In Wireless Sensor Networks:Attack and Countermeasures. International confrance in Canada. (2003). 21-24 May Canada

[9] Razzaque, M., et al. (2013). Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead. Wireless Networks and Security, Springer: 107-132.